King County
Information Technology Governance Standards

Title	Document Code No.
NETWORK INFRASTRUCTURE POLICY	ITG-P-06-03-1
Chief Information Officer Approval / Date	Effective Date.
11-7-06	

1.0 PURPOSE:

This document establishes responsibility and authority for ownership, acquisition and management of physical components of the county network infrastructure. This infrastructure must support different sets of business needs at diverse locations throughout the county. The goal of this policy is to ensure consistency in the network architecture and to ensure network components meet established technical standards.

2.0 APPLICABILITY:

This policy applies to all King County employees. It also applies to consultants and contractors providing services for the county. It is intended to focus primarily on those county employees who will be responsible for supporting information technology within their respective office, department or division.

3.0 REFERENCES:

3.1 Physical Infrastructure Standard

3.2 Network Equipment Standard

3.3 Network Configuration Standard

3.4 Wireless Networking Standard

3.5 IT Equipment Replacement Guidelines

3.6 Internal Network Protocol Standard

3.7 Network Naming and Numbering Standard

4.0 DEFINITIONS:

4.1 **County Enterprise Network**: The network commonly used to conduct county business that provides transport of data within and between county facilities and other agencies of county government. This definition also refers to the network used to transport data between the county, other government agencies and the Internet. It does not refer to networks built for the sole purpose of meeting special operations needs of county business units which include, but are not limited to process control and supervisory control networks. Nor does it refer to the King County Institutional Network (I-Net) that is required to meet contractual obligations with I-Net customers and the local cable television utility.

4.2 **Network Infrastructure Equipment:** Equipment that enables network connections for a facility, group or individual to other points on the County Enterprise Network.

This definition includes LAN switches, routers and wireless access points serving each facility and those used to aggregate and distribute data destined to other parts of the network. It also includes appliances used to control network traffic and secure the network from unauthorized access. The appliances include, but are not limited to; network traffic shapers, network firewalls, VPN concentrators and network intrusion sensors.

4.3 **Agency:** County office, division or department of the King County Assessor, Office of the Prosecuting Attorney, King County Sheriff, or the executive, legislative or judicial branches.

5.0 POLICIES:

5.1 Specification of communications cabling and its distribution within county facilities will be the responsibility of the Office of Information and Resource Management (OIRM). Requests for communications cabling will be directed to OIRM for review of needs, development of plans, approval of plans and coordination of installation. A **Physical Infrastructure Standard** will be maintained that describes current accepted general specifications for cabling, cable termination, cable spaces, distribution frames, their physical surroundings and support systems. OIRM will own this standard.

5.2 All network infrastructure equipment on the County Enterprise Network will be owned and operated by OIRM.

5.3 Plans for implementing new local area networks (LANs) and plans for expansion of existing LANs are to be reviewed and approved by OIRM prior to implementation.

5.4 A list of supported Network Infrastructure Equipment that is allowed to reside on the County Enterprise Network will be maintained and described in the **Network Equipment Standard**. Network Infrastructure Equipment to be installed on the County Enterprise Network must comply with this standard. OIRM will own this standard.

5.5 Network Infrastructure Equipment will be configured in accordance with approved templates that will be maintained in the **Network Configuration Standard**. OIRM will own this standard.

5.6 All wireless local area network (WLAN) equipment attached to the County Enterprise Network must comply with the **Network Equipment Standard**. WLAN equipment must additionally meet technical requirements described in the **Wireless Networking Standard**. OIRM will own this standard.

5.7 All Network Infrastructure Equipment is to be examined for possible replacement using steps recommended in the **IT Equipment Replacement Guidelines**. OIRM will own the OIRM Equipment Replacement Guidelines.

5.8 Network protocols used to transport traffic on the County Enterprise Network will be restricted according to rules described in the **Internal Network Protocol Standard.** The standard will describe currently authorized protocols and ways of complying with this policy when use of unauthorized protocols cannot be avoided. All new applications must comply with this standard. OIRM will own this standard.

5.9 Network addressing will be centrally administered by OIRM. Only addressing assigned by OIRM may be used in configuring equipment for operation on the network. In addition, an equipment naming convention will be followed. Standards describing acceptable methods of naming and addressing Network Infrastructure Equipment, computers, and other network attached devices will be described in the **Network Naming and Numbering Standard**. OIRM will own this standard.

5.10 Exceptions to this policy may be granted by submitting a request in writing to the Chief Information Officer (CIO) as described in the **Countywide Information Technology Policy Governance Framework.**

5.11 Proposals for changes to this policy will be received from agencies and the CIO and will be reviewed for completeness and business impacts by the **Network Policy and Standards Development Team** annually.

5.12 The CIO will review annually the status of agency adoption and compliance of this policy and the referenced standards with IT governance members.

6.0 RESPONSIBILITIES:

6.1 The CIO is the approval authority for the **Network Infrastructure Policy**.

6.2 Managers in charge of information technology within each agency or IT Service Delivery Managers are responsible for ensuring that devices, systems and applications under their control are in compliance with the **Network Infrastructure Policy.**

6.3 OIRM is responsible for protecting the integrity of the enterprise network. To meet this responsibility OIRM will ensure compliance with the terms detailed in the **Network Infrastructure Policy.**

7.0 POLICY GUIDELINES:

7.1 None